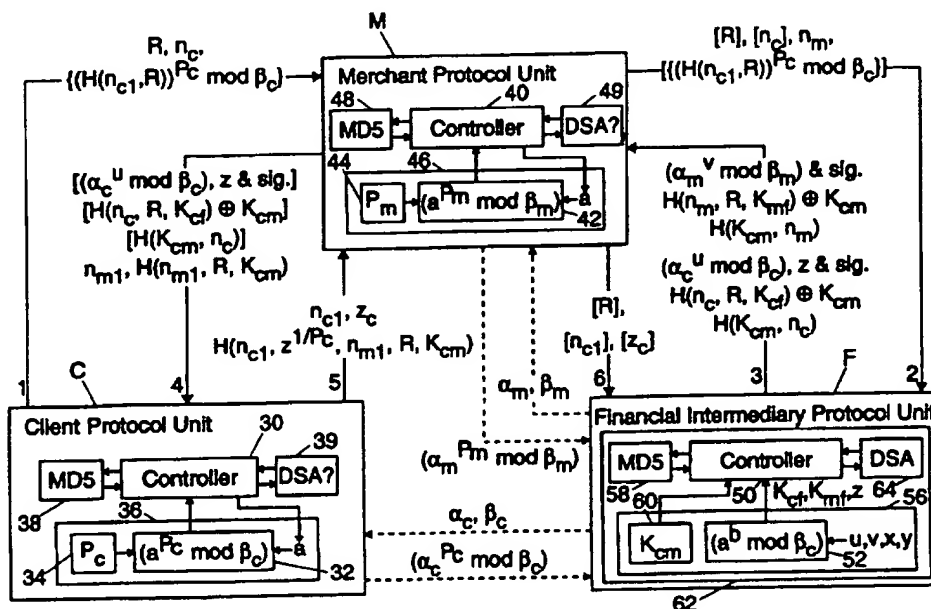




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>H04L 9/32</b>		A1	(11) International Publication Number: <b>WO 96/33568</b>
		(43) International Publication Date: 24 October 1996 (24.10.96)	
(21) International Application Number: PCT/GB96/00915		(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 17 April 1996 (17.04.96)		<b>Published</b> <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(30) Priority Data: 9507885.3      18 April 1995 (18.04.95)      GB			
(71) Applicant (for all designated States except US): HEWLETT-PACKARD COMPANY [US/US]; 3000 Hanover Street, Palo Alto, CA 94304 (US).			
(72) Inventor; and (75) Inventor/Applicant (for US only): MAO, Wenbo [CN/GB]; 60 Wheatfield Drive, Bradley Stoke, Bristol BS12 9DD (GB).			
(74) Agent: COKER, David, Graeme; Hewlett-Packard Limited, Intellectual Property Section, Building 2, Filton Road, Stoke Gifford, Bristol BS12 6QZ (GB).			

(54) Title: METHODS AND APPARATUS FOR AUTHENTICATING AN ORIGINATOR OF A MESSAGE



## (57) Abstract

Authentication by an intermediary F (e.g. a bank) of an originator C of a message (e.g. a client sending an instruction to pay a merchant M) is accomplished using a protocol which does not require the intermediary to possess passwords used by the originator C and the merchant M to protect the contents of the message. Furthermore, the protocol does not require any party to the transaction to decrypt any value previously encrypted by any other party, so a reversible encryption algorithm is not required.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

Methods and apparatus for authenticating an originator of a message

Technical Field

This invention relates to methods and apparatus for authenticating an originator of  
5 a message, and which in particular enable the originator of a message to be authenticated  
without the need for specialized authentication organizations, and without decryption of  
encrypted information.

Background Art

10 Modern computing and telecommunication systems have enabled a rapid and  
continuing increase in exchange of information between individuals and organizations, e.g.  
via the system commonly known as the Internet. However, the full potential of such  
systems is currently restricted by the difficulty of providing secure transfer of valuable  
information over the system. Many organizations would like to use publically-accessible  
15 networks for conducting various transactions, such as the sale of goods and services. In  
principle payment for such transactions could be obtained from a customer by transfer over  
the network of relevant information such as credit card details. However it is clearly  
possible for a dishonest third party to intercept such information during transmission, and  
then mis-use it to the third party's financial advantage. Various other fraudulent activities  
20 are possible, such as false repudiation of orders. Accordingly most transactions which may  
be initiated over a network still have to be completed using conventional methods such as  
exchange of paper invoices and payments or voice messages, using more trusted systems  
such as mail or voice telephone networks.

It is essential for an effective electronic transaction mechanism to have several  
25 properties:

- authentication (i.e. confirmation of origin) of messages involved in a transaction;
- protection of the integrity of messages involved in the transaction, and ability to prove if  
a message has been corrupted;
- prevention of false repudiation of an agreement to make a payment;
- 30 - prevention of frauds involving recording and replaying of messages involved in a  
transaction;
- economy of implementation; and
- compatibility with national security interests.

Various proposals have been made for electronic message authentication. Although  
35 they tend to satisfy the primarily technical requirements, they also tend to be either costly  
and/or contrary to national security interests. Thus many proposals involve reliance on a  
specialized third-party security service, for example for authentication of messages in each  
transaction or to supply and certify public encryption keys. In addition many of these

proposals involve the use of reversible encryption algorithms, i.e. algorithms in which information is concealed by encryption by a sender and retrieved again by decryption by the recipient. Such algorithms can also be used for transfer of other information which is contrary to national security interests, so the distribution and in particular export from  
5 some countries of products which incorporate reversible encryption algorithms is often controlled or prohibited. Any proposal which involves decryption, and thus requires a reversible encryption algorithm, is unlikely to be suitable to be made available for use on a widespread basis.

It is an object of this invention to provide a method and apparatus for authenticating  
10 messages which avoids the problems entailed in prior proposals, and in particular does not require any specialist security service nor involve the use of a reversible encryption technique.

#### Disclosure of Invention

15 According to one aspect of this invention there is provided a method for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values, but which does not enable the input value to be readily determined from the protected version in  
20 combination with either of said values individually, comprising the steps of:

- a) receiving a protected version of a password, said protected version being derived from a first of said component one-way functions using said password as said respective value;
- b) generating another value;
- 25 c) generating a protected version of said other value by applying a second of said component one-way functions;
- d) generating a digital signature for the protected version of said other value;
- e) applying said second component one-way function using said other value to said protected password to derive a ticket key;
- 30 f) generating a session key;
- g) protecting said session key with said ticket key;
- h) supplying said protected version of said other value, said digital signature and said protected session key to the source of said protected password; and
- i) thereafter destroying said other value, said ticket key and said session key.

35 According to one aspect of this invention there is provided apparatus for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values, but which does

not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising:

- means for receiving a protected version of a password, said protected version being derived from a first of said component one-way functions using said password as said  
5 respective value;
- means for generating another value;
- means for generating a protected version of said other value by applying a second of said component one-way functions;
- means for generating a digital signature for the protected version of said other  
10 value;
- means for applying said second component one-way function using said other value to said protected password to derive a ticket key;
- means for generating a session key;
- means for protecting said session key with said ticket key;
- 15 means for supplying said protected version of said other value, said digital signature and said protected session key to the source of said protected password.

#### Brief Description of Drawings

Methods and apparatus for authenticating an originator of a message in accordance  
20 with this invention without the use of a reversible encryption algorithm will now be described, by way of example, with reference to the accompanying drawings, in which:

- Figure 1 illustrates a transaction in which authentication of messages is necessary;
- Figure 2 is a block schematic diagram showing the transfer of messages in a  
25 protocol by which a trusted intermediary F enables two parties C and M to authenticate each other, and verifies that C has authorized a transaction; and

Figures 3a-c show successive stages of the protocol.

#### 30 Best Mode for Carrying Out the Invention, & Industrial Applicability

Referring to Figure 1, the invention will be described by reference to the example of a client 10 who wishes to instruct a financial intermediary 12 (such as a bank or credit card company) to make a payment to the account of a merchant 14. Each of these parties possesses a protocol unit C, F and M respectively, comprising for example appropriately-  
35 programmed computers (as in the case of the client 10 and the financial intermediary 12) or special-purpose hardware devices (as in the case of the merchant 14). These units are coupled to a communication system 16 which comprises multiple computer networks 18 interconnected by routers 20 and which typically serves many tens of thousands of users.

The networks 18 are of the kind in which at least some units attached to one network 18 can monitor messages travelling over that network between other units on the same or other networks 18. Accordingly it is not safe to transfer information such as financial transaction details in clear form over the system 16 in view of the risk of interception and  
 5 misuse of that information by other parties. Furthermore, the large number of people and organizations connected to the system 16 means that for any given transaction the parties involved may never have previously had any contact. Accordingly they do not necessarily have any established relationship by means of which they might confirm each other's identity and trustworthiness. Even if such a relationship does exist there remains the risk  
 10 of a fraudster masquerading as one of the parties in order to defraud the other.

The present invention provides a protocol by which the parties to a transaction, for example, can authenticate messages (i.e. confirm the origin of the messages) involved in the transaction. The method does not require the parties to share any information which one party must encode and the other must decode, for example to confirm identity; thus  
 15 there is no need for a reversible encryption algorithm to be used. Although the method does entail the participation of a trusted intermediary, many existing transactions typically involve the participation of such an intermediary in the form of a financial institution, in which trust is placed, so this requirement should not normally constitute an obstacle. Furthermore the intermediary does not have to hold secret information belonging to either  
 20 party.

The protocol involves the use of an arithmetic operation known as modular exponentiation, in which a first number  $\alpha$  is raised to some power  $p$ , and this value is divided by a second number  $\beta$ ; the desired result  $q$  is the remainder of the division operation:

$$25 \quad q = \alpha^p \bmod \beta \quad (1)$$

Modular exponentiation is a one-way function, in that although the operation of equation (1) is straightforward to perform, the inverse operation, i.e. determination of  $p$  given  $\alpha$ ,  $\beta$  and  $q$ , can be made extremely hard by appropriate choice of the values of  $\alpha$  and  $\beta$ .  $\beta$  is chosen to satisfy the condition

$$30 \quad \beta = 2i + 1 \quad (2)$$

where  $i$  is a prime number.  $\alpha$  is typically chosen to be a value which is a 'generator modulo  $\beta$ ', meaning that the value of  $(\alpha^p \bmod \beta)$  varies through all values between 1 and  $\beta-1$  as  $p$  varies between 1 and  $\beta-1$ . Pairs of values  $\alpha$ ,  $\beta$  can be selected so that  $\beta$  conforms to equation (2), for example using the method described in *Applied Cryptography*  
 35 by B. Schneier, John Wiley & Sons, 1994, pp. 208-9.

Referring to Figure 2, it is first necessary for the client 10 and the merchant 14 to select respective passwords  $P_c$  and  $P_m$ , and for these to be notified in encoded form to the financial intermediary 12 once only prior to the first transaction. To this end the financial

intermediary's protocol unit F selects pairs of numbers  $\alpha_c$ ,  $\beta_c$  and  $\alpha_m$ ,  $\beta_m$  as described above, stores them for future use as described below, and informs the client's protocol unit C and the merchant's protocol unit M respectively of the values of these pairs, as indicated by dashed lines 22 and 24. No particular secrecy or security is required for this step.

- 5 Thus the values may be sent in printed form by mail, and entered into the protocol units via a keyboard, magnetic stripe card or the like. The client 10 selects a password (e.g. an easily memorized word, number, etc.) and enters this into the protocol unit C as well. The unit C manipulates this password in a predetermined manner to convert it to purely digital form if necessary and ensure the resulting value  $P_c$  is in one of the ranges [3,  $i-1$ ]  
10 and [ $i+1$ ,  $\beta_c-2$ ], where  $i$  satisfies the relation  $\beta_c = 2i+1$ , so that the value of  $P_c$  is relatively prime to  $\beta_c-1$ . The digital password  $P_c$  is then encoded by hashing it using equation (1) and the numbers  $\alpha_c$ ,  $\beta_c$  supplied by the financial intermediary 12

$$E_{P_c} = \alpha_c^{P_c} \bmod \beta_c \quad (3)$$

- If desired, to decrease vulnerability to guessing etc. of the client's selected password by  
15 another person, the digital password  $P_c$  may be concatenated with a random 'salt' value  $s$  before encoding, as described in *Unix operating system security* by F.T. Grampp and R.H. Morris, AT&T Bell Laboratories Technical Journal, 63, October 1984. In this case the encoding operation is

$$E_{P_c} = \alpha_c^{sP_c} \bmod \beta_c \quad (3a)$$

- 20 The encoded value  $E_{P_c}$  is communicated to the financial intermediary 12 by the client's protocol unit C, as indicated by dashed line 26, taking reasonable precautions to verify the association of the value of  $E_{P_c}$  with the client.

- In order to implement and coordinate these functions the client's protocol unit C includes a controller 30 coupled to an exponentiation unit 32, and a module 34 for deriving  
25 the digital password  $P_c$  from the client's password and for supplying it to the exponentiation unit. This unit is arranged to perform the calculation

$$a^{P_c} \bmod \beta_c \quad (4)$$

- on any value  $a$ , including  $\alpha_c$ , supplied to it by the controller 30, and to furnish the result of this calculation to the controller. For security purposes the storage module 34 and the  
30 exponentiation unit 32 are designed never to output the value of the password  $P_c$  directly, as indicated schematically by the enclosure 36 around them. The values  $\alpha_c$ ,  $\beta_c$  and  $s$  (if used) may be concatenated for storage purposes to make misuse by another person of the values as stored more difficult.

- The merchant likewise selects a password and enters it into the protocol unit M (for  
35 example using a smart card which is accessible to the merchant's staff). The unit M derives a corresponding digital password  $P_m$ , encodes it using the numbers  $\alpha_m$ ,  $\beta_m$  according to the relation

$$E_{P_m} = \alpha_m^{P_m} \bmod \beta_m \quad (5)$$

and communicates the value  $E_{pm}$  to the financial intermediary 12 in confidence, as indicated by the dashed line 28. The merchant's protocol unit includes a controller 40, exponentiation unit 42, storage module 44 and enclosure 46 corresponding to the items 30 to 36 in the client's unit C.

- 5 Referring to Figures 3a to 3c, in a first stage 100 of the protocol, the client 10 composes an appropriate message, such as "transfer five hundred dollars from my account no. 1234 5678 9876 to M's account no. 9876 5432 1234" and enters it into her protocol unit C. As a preliminary step to deriving a digital signature which incorporates the client's password  $P_c$  and which will accompany this message, the controller 30 in the unit 10 then  
 10 generates two numbers  $n_c, n_{c1}$ ; the values of these numbers may or may not be selected essentially at random (although with the restriction noted below in the case of  $n_{c1}$ ), but the controller 30 is arranged to ensure that each value used is chosen afresh, for each transaction, in a manner which makes it unlikely that anyone else can predict the value chosen and unlikely that the same value will be chosen for two different transactions. As  
 15 they are used on a single occasion the numbers  $n_c, n_{c1}$  are referred to as 'nonces'.

- The controller 30 concatenates the nonce  $n_{c1}$  with a digital representation R of the characters comprising the client's message, and encodes the resulting sequence of digits using a one-way hashing function (such as the MD5 function described in *The MD5 message digest algorithm* by R.L. Rivest, Internet RFC 1321, April 1992) to produce a  
 20 fixed-length sequence of digits represented herein as  $H(n_{c1}, R)$ , where H is the hashing function. The unit C includes an MD5 encoder 38 coupled to the controller 30 for effecting this hashing function. The value of  $n_{c1}$  is selected by the controller 30 so that  $H(n_{c1}, R)$  is a generator modulo  $\beta_c$ , in the same manner as described above in respect of the number  $\alpha$ . Selection of  $n_{c1}$  in this way makes it hard to discover the value of  $H(n_{c1},$   
 25 R) from the password-protected version (described below) which will actually be transmitted. The use of the hashing function H has the effect of compressing the size of the digital value involved, thereby facilitating subsequent calculations, and itself makes decoding computationally infeasible. The values of  $n_{c1}$  and thus of  $H(n_{c1}, R)$  play a significant role in the final verification of the client's digital signature, so it is important  
 30 that they are protected at this stage.

The hashed value  $H(n_{c1}, R)$  is itself password-protected by the controller 30 by supplying it as the input value  $a$  to the exponentiation unit 32, in order to derive the client's digital signature for the message R according to the relation:

$$S_c = \{(H(n_{c1}, R))^{P_c} \bmod \beta_c\} \quad (6)$$

- 35 The protocol unit C then sends the message R, the nonce  $n_c$  and the signature  $S_c$  to the merchant's protocol unit M through the communication system 16, as indicated in Figure 2 by the message transfer labelled 1.

In the next stage 102 (Figure 3a) of the protocol, the controller 40 in the protocol

unit M itself selects a nonce  $n_m$  for this transaction, and forwards it to the financial intermediary's protocol unit F, together with the message R, the nonce  $n_c$  and the signature  $S_c$  received from the protocol unit C. This is indicated in Figure 2 by the message transfer labelled 2; the items R,  $n_c$  and the signature  $S_c$  are enclosed in square brackets [ ] to  
 5 indicate that these values are not generated or re-calculated by the protocol unit M, but are simply forwarded as received.

When these items are received by the protocol unit F, it undertakes a series of steps comprising stage 104 (Figure 3a) of the protocol. To this end the protocol unit F includes a controller 50 coupled to an exponentiation unit 52 in a secure enclosure 56 in similar  
 10 manner to the client's unit C. The secure enclosure 56 also contains a session key generator 60 for producing random number keys and supplying them to the controller 50; since the security of these session keys is important, the controller 50 itself is located in a secure enclosure 62. This enclosure 62 also contains an MD5 encoder 58 corresponding to the encoder 38 in the client's unit C.

15 The steps performed in stage 104 are as follows:

(i) Generate two nonces  $u$  and  $v$  for use once only for this purpose, in the ranges

$[3, i-1]$  and  $[i+1, \beta_c-2]$  for  $u$

$[3, j-1]$  and  $[j+1, \beta_m-2]$  for  $v$

where  $i$  satisfies the relation  $\beta_c = 2i + 1$  and  $j$  satisfies the relation  $\beta_m = 2j + 1$ .

20 (ii) Compute two keys, again for use once only for the present transaction, one key  $K_{cf}$  being used by the client's unit C and the financial intermediary's unit F, and the other key  $K_{mf}$  being used by the merchant's unit M and the financial intermediary's unit F; these keys are derived by the controller 50 according to the relations:

$$K_{cf} = (E_{pc})^u \bmod \beta_c \quad (7)$$

25  $K_{mf} = (E_{pm})^v \bmod \beta_m \quad (8)$

It should be noted that the right-hand side of equation 7 can be expanded into the form

$$(\alpha_c^{P_c} \bmod \beta_c)^u \bmod \beta_c \quad (9)$$

and that, because modular exponentiation is commutative

$$K_{cf} = (\alpha_c^{P_c} \bmod \beta_c)^u \bmod \beta_c = (\alpha_c^u \bmod \beta_c)^{P_c} \bmod \beta_c \quad (10)$$

30 Thus if the client's protocol unit C is provided with the value  $E_c = (\alpha_c^u \bmod \beta_c)$ , which can be readily done without risking revealing the value of  $u$ , then the controller 30 can set  $a$  equal to this value  $E_c$  and compute the value of the key  $K_{cf}$  using formula (4) above. Equation (10) in effect defines a composite one-way function, comprising a first component one-way function  $(\alpha_c^{P_c} \bmod \beta_c)$  using the password  $P_c$ , and a second component one-way  
 35 function  $((E_{pc})^u \bmod \beta_c)$  using the value  $u$ . The merchant's protocol unit M can likewise compute the value of the key  $K_{mf}$  from the formula  $(E_m)^{P_m} \bmod \beta_m$  where  $E_m = (\alpha_m^v \bmod \beta_m)$ .

(iii) Compute the values  $E_c$  and  $E_m$ , using the number pairs  $\alpha_c, \beta_c$  and  $\alpha_m, \beta_m$ , which

the unit F originally selected, and the values  $u$  and  $v$  generated at step (i).

- (iv) Obtain a random number from the session key generator 60 for use as a session key  $K_{cm}$  which will be made known to both the client's protocol unit C and the merchant's unit M, and communicated by each unit to the other to verify the sending unit's identity. To  
 5 protect the session key itself, the controller 50 generates two encoding keys, one for the unit C and one for the unit M, using the hashing function provided by MD5 encoder 58, and combines the session key with these keys to produce two tickets by a bitwise exclusive-OR (XOR) operation, represented by  $\oplus$  in the following relationships:

$$\text{ticket for C} = H(n_c, R, K_{cf}) \oplus K_{cm} \quad (11)$$

$$10 \quad \text{ticket for M} = H(n_m, R, K_{mf}) \oplus K_{cm} \quad (12)$$

- (v) To enable the integrity of these tickets to be verified by their respective recipients, generate respective verifiers  $H(K_{cm}, n_c)$  and  $H(K_{cm}, n_m)$ , again using the hashing function provided by the MD5 encoder 58.

- (vi) In preparation for verifying the client's digital signature  $S_c$  which will subsequently  
 15 be forwarded by the merchant's protocol unit M, generate two more random numbers  $x$  and  $y$ , both in the ranges  $[3, i-1]$  and  $[i+1, \beta_c-2]$ , and use them to compute a value  $z$  according to the relationship:

$$z = \{((S_c)^x \bmod \beta_c)((E_{pc})^y \bmod \beta_c)\} \quad (13)$$

- (vii) Compute two digital signatures: one signature  $S_{FC}$  for the concatenation of the  
 20 values  $E_u$  and  $z$ ; and a second signature  $S_{FM}$  for the value  $E_u$ . These signatures are produced by using, for example, the Digital Signature Algorithm (DSA) defined in *Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)*, Federal Register, v. 56, no. 169, 30 Aug 1991, pp. 42980-42982, to enable the values of  $E_u$ ,  $z$  and  $E_v$  to be authenticated upon reception. For this purpose the unit F includes a  
 25 DSA encoder 64 located within the enclosure 62 and connected to the controller 50.

To conclude stage 104, the protocol unit F sends the following items back to the merchant's protocol unit M:

- 30  $E_u$ ,  $z$  and  $S_{FC}$  for the client's unit C;  
 $E_v$  and  $S_{FM}$  for the merchant's unit M;  
 the ticket  $H(n_c, R, K_{cf}) \oplus K_{cm}$  for C;  
 the ticket  $H(n_m, R, K_{mf}) \oplus K_{cm}$  for M;  
 the verifiers  $H(K_{cm}, n_c)$  and  $H(K_{cm}, n_m)$ .

This communication is indicated in Figure 2 by the message transfer labelled 3.

- Upon receipt of these items the merchant's protocol unit M commences stage 106  
 35 of the protocol (Figure 3b). First the controller 40 in this unit checks the received value  $E_v$  by using the associated DSA signature  $S_{FM}$ ; for this purpose the unit M includes a DSA verifier 49. Next the controller derives the value of the key  $K_{mf}$  using the merchant's password  $P_m$  in the formula  $(E_v)^{P_m} \bmod \beta_m$ . With the key  $K_{mf}$ , the digital message R

received from the client C and the nonce  $n_m$  it generated at stage 102, the controller 40 can now use the MD5 encoder 48 to obtain the hashed value  $H(n_m, R, K_{mf})$ . By using an exclusive-OR operation of this value with the ticket  $H(n_m, R, K_{mf}) \oplus K_{cm}$  defined in equation (12), the controller 40 can determine the session key  $K_{cm}$ . The integrity of this  
 5 session key is verified by obtaining the hashed value  $H(K_{cm}, n_m)$ , using the MD5 encoder 48 again, and comparing it with the corresponding hashed value sent by the protocol unit F. The inclusion of the nonce  $n_m$  in this check confirms that the session key  $K_{cm}$  has been freshly generated.

If these checks are satisfactory, the controller 40 proceeds to generate a second  
 10 nonce  $n_{m1}$  for the merchant's unit M, and then obtains a new hashed value  $H(n_{m1}, R, K_{cm})$  from the MD5 encoder 48, for use in demonstrating to the client's unit C the authenticity of the next communication it receives from merchant's unit M.

For this next communication, indicated by the message transfer labelled 4 in Figure 2, the unit M sends the following items to the unit C:

- 15  $E_a$ ,  $z$  and  $S_{FC}$  (as received from the unit F);  
 the ticket  $H(n_c, R, K_{cf}) \oplus K_{cm}$  (as received from the unit F);  
 the verifier  $H(K_{cm}, n_c)$  (as received from the unit F);  
 the nonce  $n_{m1}$  and the new hashed value  $H(n_{m1}, R, K_{cm})$ .

In the next stage 108 of the protocol, the controller 30 in the unit C performs  
 20 several steps analogous to those just performed in the unit M: it checks the received value  $E_a$  by using the associated DSA signature  $S_{FC}$ , for which purpose it includes a DSA verifier 39. Next the controller 30 derives the value of the key  $K_{cf}$  using the client's password  $P_c$  and with  $a$  set to the value  $E_a$  in formula (4) above. With the key  $K_{cf}$ , the digital message  $R$  and the nonce  $n_c$  it generated, the controller 30 can now use the MD5 encoder 38 to  
 25 obtain the hashed value  $H(n_c, R, K_{cf})$ . By using an exclusive-OR operation of this value with the ticket  $H(n_c, R, K_{cf}) \oplus K_{cm}$  defined in equation (11), the controller 30 can determine the session key  $K_{cm}$ . The integrity of this session key is verified by obtaining the hashed value  $H(K_{cm}, n_c)$ , using the MD5 encoder 38 again, and comparing it with the corresponding hashed value sent by the protocol unit F via the merchant's unit M. The  
 30 inclusion of the nonce  $n_c$  in this check confirms that the session key  $K_{cm}$  has been freshly generated.

With this session key and the nonce  $n_{m1}$ , the controller 30 now obtains from the MD5 encoder 38 the hashed value  $H(n_{m1}, R, K_{cm})$ , and compares it with the hashed value received from the merchant's protocol unit M. If this comparison is successful, indicating  
 35 that the merchant 14 is in possession of the session key  $K_{cm}$ , the authenticity of the communication from the merchant 14 has been confirmed. Accordingly the client's unit C can proceed with authorization of the transaction.

To this end, in the final part of stage 108 (Figure 3c), the controller 30 derives the

following value to enable the financial intermediary to confirm the client's signature undeniably:

$$z_c = z^{1/P_c} \bmod \beta_c \quad (14)$$

where  $1/P_c$  indicates the inverse of the password  $P_c$  modulo  $(\beta_c-1)$ , derived from  $P_c$  as described in *Cryptography and Data Security* by D.E. Denning, Addison-Wesley, 1982.

The controller 30 then obtains from the MD5 encoder 38 the hashed value  $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$  and sends it, with the value  $z_c$  and the nonce  $n_{c1}$  which was included in the digital signature  $S_c$ , to the merchant's protocol unit M, as indicated by the message transfer labelled 5 in Figure 2.

At stage 110, the controller 40 in the unit M then obtains from the MD5 encoder 48 the hashed value  $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$  and compares it with the value received from the unit C. If the comparison is correct, indicating that the client 10 is also in possession of the session key  $K_{cm}$  together with the message R, the authenticity of the communication from the client 10 has been confirmed. Accordingly the merchant's unit M forwards the client's confirmation of the digital signature  $S_c$  by sending the items R,  $n_{c1}$  and  $z_c$  to the protocol unit F, as indicated by the message transfer labelled 6 in Figure 2.

In the final stage 112 of the protocol, the protocol unit F, now having the nonce  $n_{c1}$ , obtains the hashed value  $H(n_{c1}, R)$  from the MD5 encoder 58, and verifies the client's digital signature  $S_c$  by checking whether the following relationship is satisfied:

$$z_c = \{((H(n_{c1}, R))^* \bmod \beta_c)(\alpha_c^? \bmod \beta_c)\} \quad (15)$$

If this relationship is satisfied, the signature is confirmed as being genuine, and cannot be repudiated (as explained below).

This protocol establishes the following facts for the financial intermediary F:  
the authenticity of the client's signature;

both the client's unit C and the merchant's unit M have correctly used their keys  $K_{cf}$  and  $K_{mf}$ ;

both the client's unit C and the merchant's unit M have correctly used the session key  $K_{cm}$ , and they each have established that the other has correctly used it (i.e. they have each authenticated the other's identity);

these authentications relate to the message R;

by sending the nonce  $n_{c1}$  to the financial intermediary's protocol unit F, via the merchant's unit M, the client 10 has confirmed her agreement to the contents of the message R.

The protocol accomplishes these demonstrations by means of authentication performed by the trusted intermediary 12; however, it is not necessary for the intermediary F to possess the passwords  $P_c$  and  $P_m$  of the client 10 and the merchant 14: the relevant encryption is performed without the encryption function being directly available to the intermediary F. Furthermore, inspection of the protocol shows that

nowhere is it necessary for any unit C, M or F to decrypt any value previously encrypted by any other unit. Thus there is no need to use a reversible encryption algorithm of a kind which would be subject to regulatory restrictions (typically an exclusive-OR operation is not regarded as falling into a restricted category).

- 5 In particular the protocol involves the use of two nonces ( $u$  and  $v$ ), in a manner which does not require them to be communicated as such. Furthermore, the manner in which they are communicated (incorporated into the values  $E_u$  and  $E_v$ ) does not enable them to be readily discovered, and the information they protect ( $K_{ct}$  and  $K_{cm}$ ) is not communicated as such, although it can be obtained by parties properly possessing the  
10 appropriate passwords  $P_c$  and  $P_m$  without those parties needing to know the values  $u$  and  $v$  themselves. Digital signatures  $S_{FC}$  and  $S_{FM}$  are supplied with the values  $E_u$  and  $E_v$  to authenticate them, and are used for that purpose only. Accordingly, it is relatively easy and economical to implement a very secure, tamper-resistant device (i.e. the protocol unit F) to generate the one-time numbers  $u$  and  $v$ , compute the values  $E_u$  and  $E_v$ , and sign them  
15 digitally with the signatures  $S_{FC}$  and  $S_{FM}$ .

- If it is necessary to prove that the digital signature  $S_c$  did originate from the client  
10, this can be done by requesting the client to provide the result of the formula (4) for one hundred different numbers  $a$ . Ninety-nine of these numbers are chosen to have the form  $(\alpha_c^x \bmod \beta_c)$ , i.e. are derived from ninety-nine values of  $x$ , so the results provided  
20 by the client 10 can be checked by performing the calculation

$$((E_{P_c})^a \bmod \beta_c) \quad (16)$$

If these ninety-nine results are correct, the client 10 is shown to have used her password  $P_c$  in obtaining them.

The remaining value  $a$  is derived using the formula

$$25 \quad (\alpha_c^b \bmod \beta_c)(H(n_{ci}, R)) \quad (17)$$

where  $b$  is selected from the ranges  $[3, i-1]$  and  $[i+1, \beta_c-2]$ . The result  $d$  provided by the client 10 from formula (4) is tested using the relationship

$$d = [S_c((E_{P_c})^b \bmod \beta_c)] \bmod \beta_c \quad (18)$$

- If this relationship is satisfied, the digital signature  $S_c$  must have been produced using the  
30 client's password  $P_c$ .

## CLAIMS

1. A method for enabling authentication of an originator of a message, using a  
5 composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values ( $u$ ,  $P_j$ ), but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising the steps of:
  - 10 a) receiving a protected version ( $E_{P_c}$ ) of a password ( $P_j$ ), said protected version being derived from a first of said component one-way functions using said password ( $P_j$ ) as said respective value;
  - b) generating another value ( $u$ );
  - c) generating a protected version ( $E_u$ ) of said other value by applying a second of said  
15 component one-way functions;
  - d) generating a digital signature ( $S_{FC}$ ) for the protected version ( $E_u$ ) of said other value;
  - e) applying said second component one-way function using said other value ( $u$ ) to said protected password ( $E_{P_c}$ ) to derive a ticket key ( $K_{ct}$ );
  - f) generating a session key ( $K_{cm}$ );
  - 20 g) protecting said session key ( $K_{cm}$ ) with said ticket key ( $K_{ct}$ );
  - h) supplying said protected version ( $E_u$ ) of said other value, said digital signature ( $S_{FC}$ ) and said protected session key ( $K_{cm}$ ) to the source of said protected password ( $E_{P_c}$ ); and
  - i) thereafter destroying said other value ( $u$ ), said ticket key ( $K_{ct}$ ) and said session key ( $K_{cm}$ ).
- 25 2. The method of claim 1, wherein said component one-way functions incorporate modular exponentiation.
3. The method of claim 1 or claim 2, wherein said session key is protected with said  
30 ticket key by a bitwise exclusive-OR operation.
4. Apparatus for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two  
35 respective values ( $u$ ,  $P_j$ ), but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising:
 

means for receiving a protected version ( $E_{P_c}$ ) of a password ( $P_j$ ), said protected

## 13

- version being derived from a first of said component one-way functions using said password ( $P_c$ ) as said respective value;
- means for generating another value ( $u$ );
- means for generating a protected version ( $E_u$ ) of said other value by applying a
- 5 second of said component one-way functions;
- means for generating a digital signature ( $S_{FC}$ ) for the protected version ( $E_u$ ) of said other value;
- means for applying said second component one-way function using said other value ( $u$ ) to said protected password ( $E_{Pc}$ ) to derive a ticket key ( $K_{ct}$ );
- 10 means for generating a session key ( $K_{cm}$ );
- means for protecting said session key ( $K_{cm}$ ) with said ticket key ( $K_{ct}$ );
- means for supplying said protected version ( $E_u$ ) of said other value, said digital signature ( $S_{FC}$ ) and said protected session key ( $K_{cm}$ ) to the source of said protected password ( $E_{Pc}$ ).

15

1/5

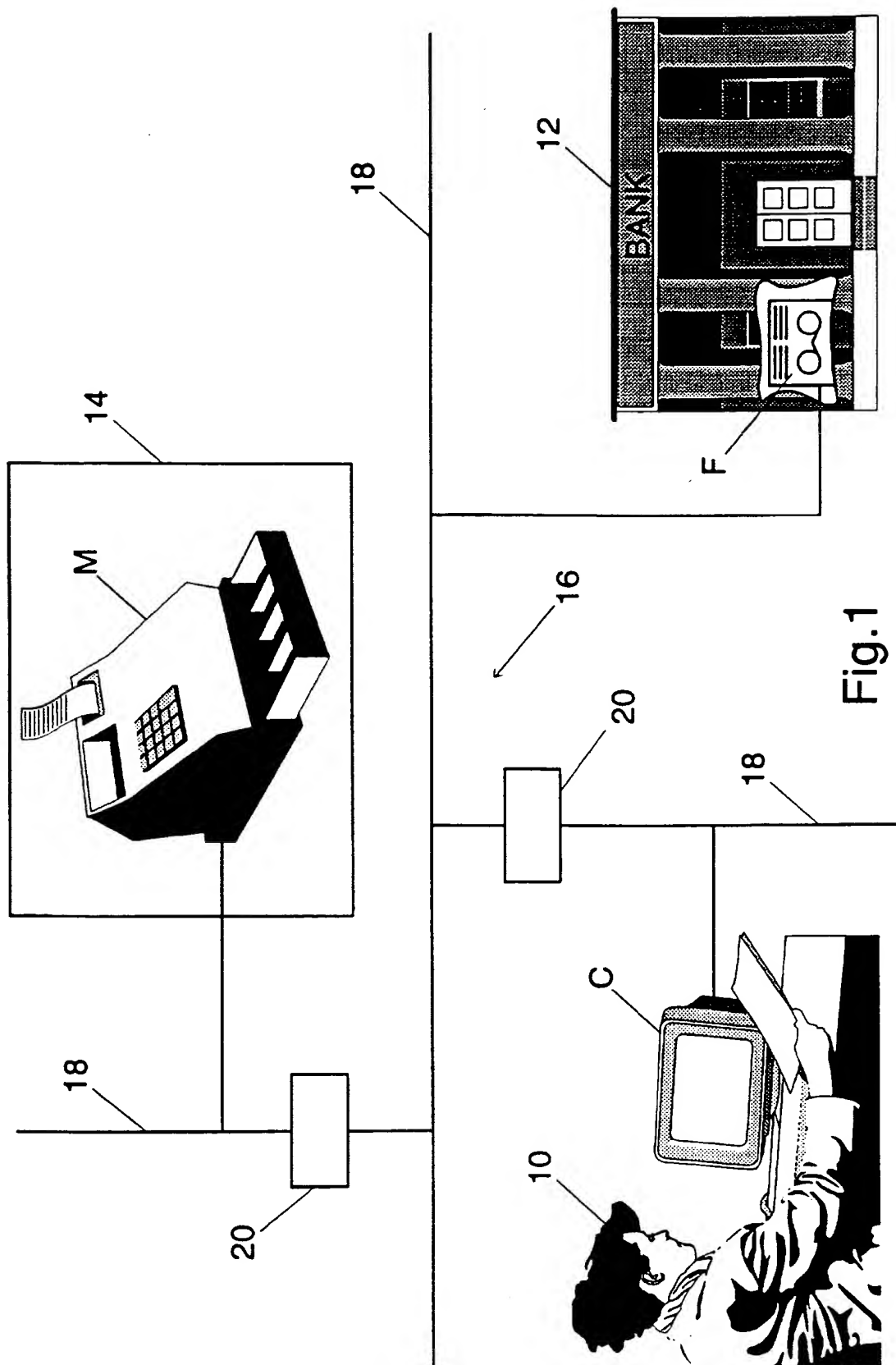
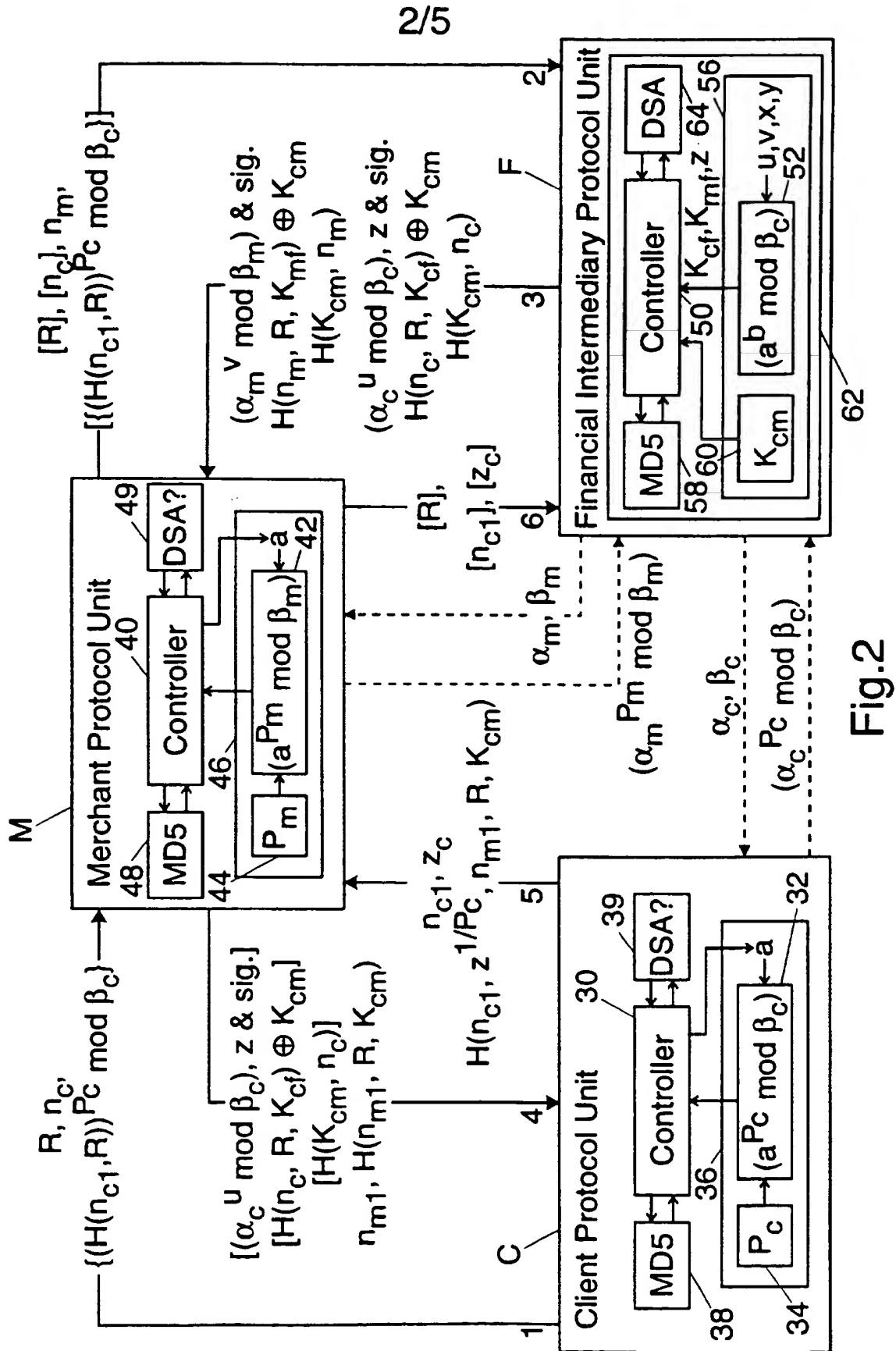
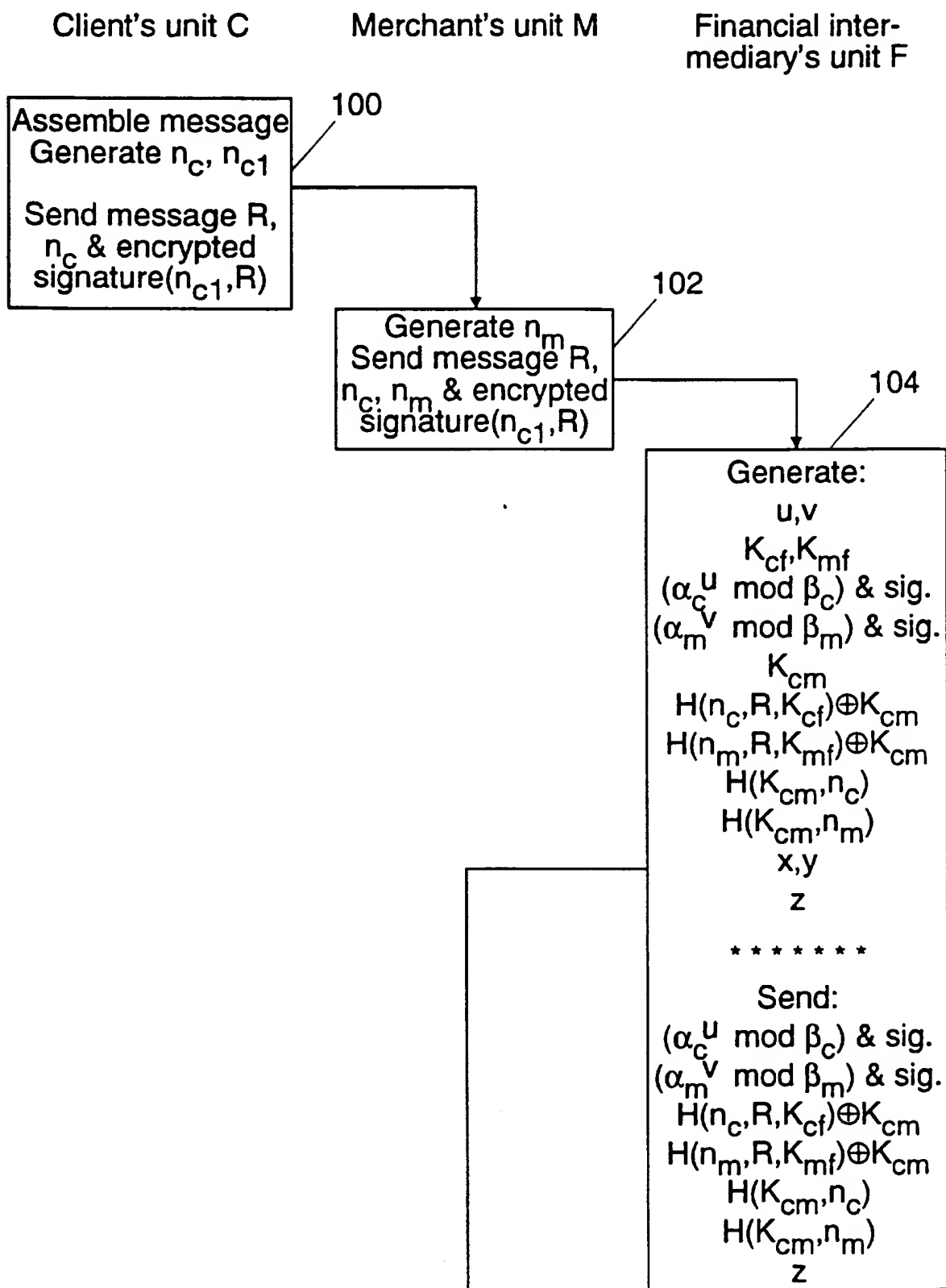


Fig. 1



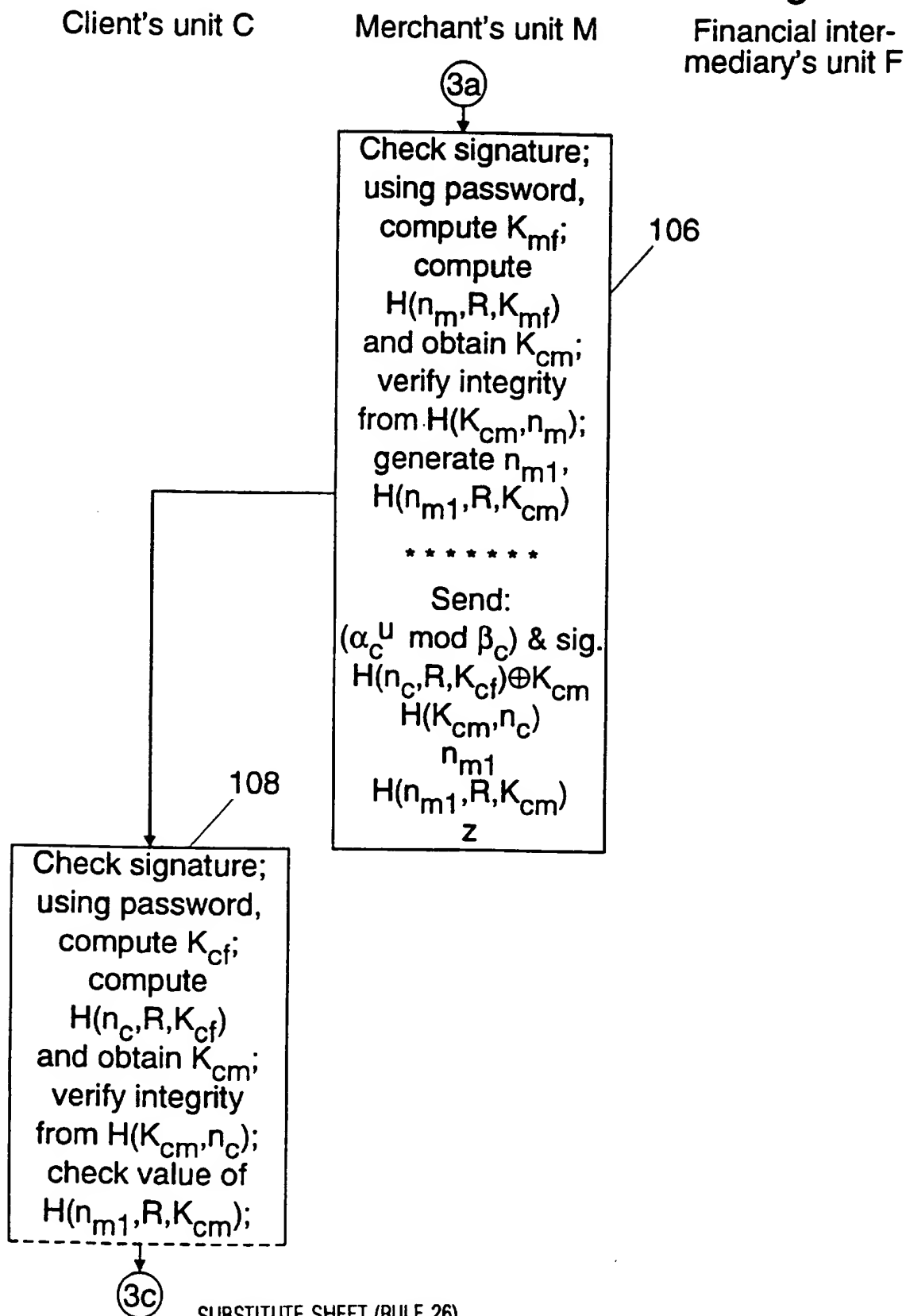
3/5

Fig.3a



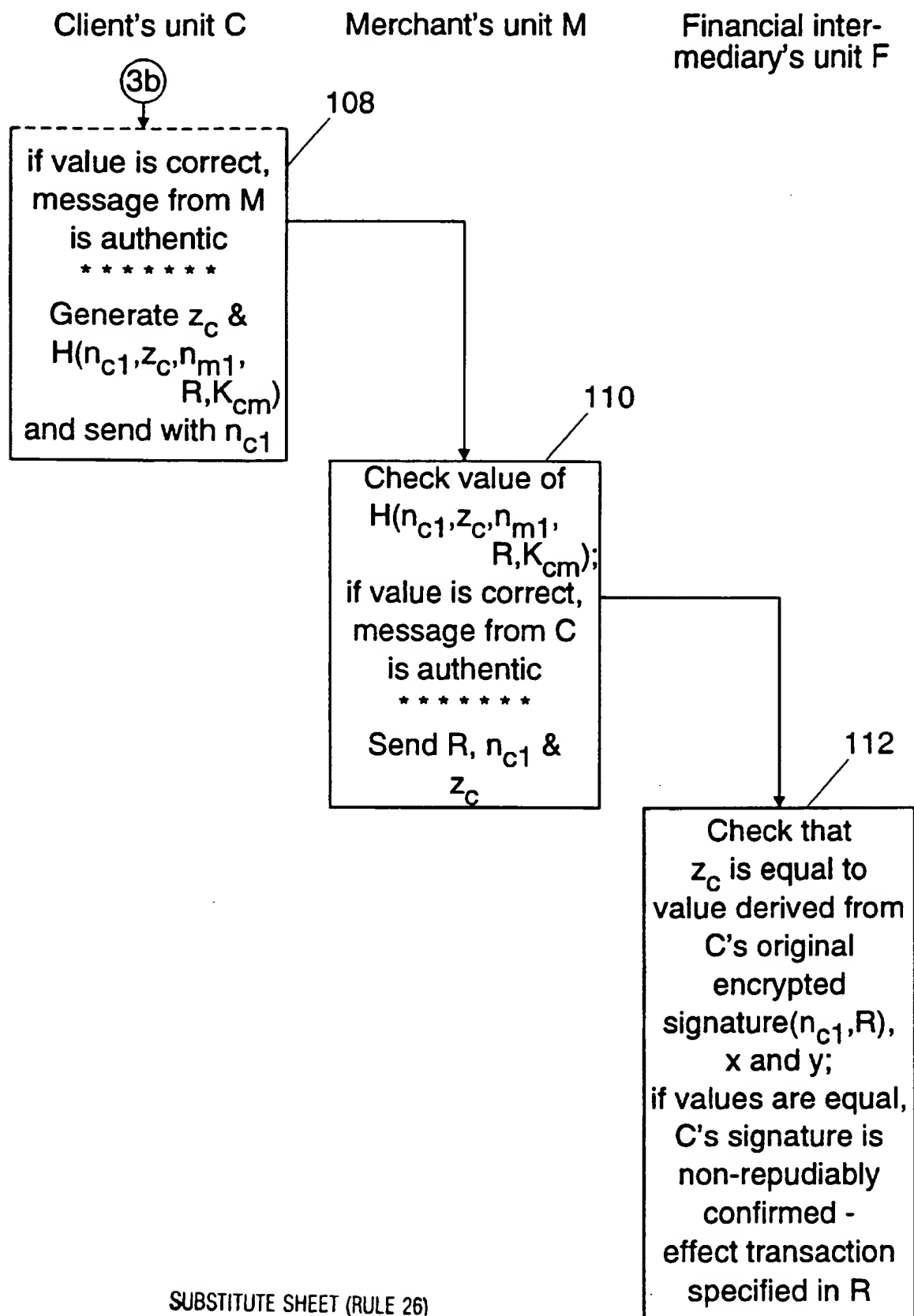
4/5

Fig.3b



5/5

Fig.3c



## INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 96/00915

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,91 14980 (SIEMENS NIXDORF) 3 October 1991 see page 5, line 22 - line 31 see page 6, line 5 - line 16 see page 6, line 30 - line 32 see page 8, last paragraph - page 9, line 21 see page 10, line 3 - page 11, line 12 see page 14, paragraph 1 ---	1,2,4
A	OPERATING SYSTEMS REVIEW, JAN. 1987, USA, vol. 21, no. 1, ISSN 0163-5980, pages 8-10, XP002008756 OTWAY D ET AL: "Efficient and timely mutual authentication" see page 9, left-hand column, line 1 - page 10, left-hand column, last line -----	1,4



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*&\* document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 1996	12.08.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer  Holper, G

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 96/00915

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9114980	03-10-91	DE-A- 4008971	26-09-91
		EP-A- 0472714	04-03-92
		JP-T- 4504020	16-07-92
		US-A- 5323146	21-06-94
-----			